REMARKS

Claims 14-33 are pending in the present application, claims 1-13 having been cancelled herein. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

The disclosure was objected to due to a number of informalities. These informalities have been corrected by the above amendment. Withdrawal of the objection is thus respectfully requested.

Claims 4, 5, 8, 9, and 12 were objected to due to a number of informalities. The cancellation of these claims has rendered these informalities moot and withdrawal of the objection is thus respectfully requested.

Claims 1-13 were rejected under 35 U.S.C. § 101 because the claimed invention was allegedly directed to non-statutory subject matter. Claims 1-13 have been cancelled thus rendering this rejection moot. Applicant submits that new claims 14-33 comply with the requirements of 35 U.S.C. § 101. The claims now recite, *inter alia*, first and second electronic entities. Thus, the claims recite an invention which results in a practical application producing a concrete useful and tangible result to form the basis of statutory subject matter under 35 U.S.C. § 101. Withdrawal of this rejection is respectfully requested.

Claims 1-13 were rejected under 35 U.S.C. § 112, second paragraph. Again, Applicants have cancelled claims 1-13, thus rendering this rejection moot. Applicants submit that new claims 14-33 comply with the requirements of 35 U.S.C. § 112, second paragraph. Most notably, new claims 14-33 now specifically recite method steps that clearly describe how the cryptographic protocol is performed. Withdrawal of the rejection is thus respectfully requested.

Claims 1-13 were rejected under 35 U.S.C. § 102(e) as being anticipated by Kocher et al (U.S. Patent No. 6,278,783). This rejection is respectfully traversed for the following reasons.

Claims 1-13 have been cancelled, in favor of new claims 14-33. Claims 14-19 substantially correspond to old claims 1-6. Claims 20 and 21 are new and intended to cover the general features of Fig. 2 (claim 21 adding to claim 20 that the step of randomly selecting to perform in normal state or complemented state occurs for each operation of the at least a part of the first chain of operations). Claims 22, 23, 31, and 32 correspond substantially to old claims 7 and 8. Claims 24 and 33 correspond to old claim 10, in the case of claims 20 and 21, i.e., in the case of Fig. 2. Claim 25 substantially corresponds to old claim 9, i.e. to the case of Fig. 1. Claim 26 corresponds substantially to old claim 10,

in the case of claim 25, i.e. in the case of Fig. 1. Claims 27 and 28 substantially correspond to old claims 11 and 12 and claims 29 and 30 substantially correspond to old claim 13, split in two (claim 29 dealing with permutation of communitative operations, and claims 30 adding that such permutation is random).

Claim 14 recites a method of performing a cryptographic protocol between a first electronic entity and a second electronic entity in order to resist to an attack against the second electronic entity. The method comprises the steps of: applying a message to both first and second electronic entities, applying a first chain of operations to the message within the first electronic entity, so as to obtain a result, and determining a second chain of operations derived from the first chain of operations and applying the second chain of operations to the message within the second electronic entity so as to obtain a resultant message. The step of determining the second chain of operations comprises randomly selecting, for at least a part of the operations of the first chain of operations, to perform either the at least a part of the operations of the first chain of operations or the at least a part of the first chain of operations in a complemented state.

The method further comprises the steps of outputting as the resultant message, responsive to the step of randomly selecting, one of either a last operation of the first chain of operations, or a complemented result of a second chain of operations, and comparing the resultant message to the result. This is not taught, disclosed or made obvious by the prior art of record.

Applicant respectfully submits that Kocher concerns a method according to which a message, before being processed, is randomly split into two parts, wherein the key is randomly split into two parts as well. Kocher fails to teach or suggest to either operate a given chain of operations, either in a normal state or in a complemented state. Thus, this reference does not refer to any random selection between operations performed either in a normal state or in a complemented state. Accordingly, Applicant submits that claim 14 is patentable over Kocher.

Claims 15-33 depend from and include the recitations of claim 14. Applicant respectfully submits that these claims are patentable over the prior art at least for the reasons discussed above with respect to claim 14.

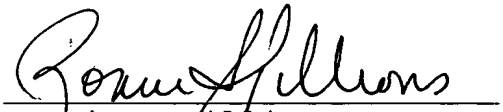
In view of the above amendments and remarks, Applicant respectfully requests reconsideration and withdrawal

of the outstanding rejections of record. Applicant submits that the application is in condition for allowance and early notice to this effect is most earnestly solicited.

If the Examiner has any questions he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant

By 
Ronni S. Jillions
Registration No. 31,979

RSJ:tbs
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\B\Bonn\Akkarl\pto\19Jan2005AMD.doc